

Traffic Analysis of Mark Angel Store

Date: August 1, 2025

Tool Used: Wireshark

Focus: TCP Handshake Validation | TLS Session Initiation | Host Attribution

Objective

To conduct a structured forensic analysis of encrypted web traffic between a client machine and the Markangel Stores web server, focusing on handshake validation, TLS session initiation, and IP attribution.

Scope of Work:

This analysis reviewed a PCAP capture involving access to the Markangel Stores website. The primary objective was to dissect the early stages of the communication, emphasising the TCP three-way handshake and the start of encrypted (TLS) traffic. The session was assessed to determine the legitimacy of the connection, the identities of the client and server, and the nature of encrypted communication.

Key Findings:

What is the IP address of the webserver hosting Markangel Stores?
63.250.43.1

What is the IP Address of the machine used to access the markangel website? 10.10.10.162

What is the timestamp of the TCP synchronization request made to markangel stores (YYYY-MM-DD HH:MM:SS)? 2024-10-26 11:15:17.486013

What is the source IP of the first SYN-ACK packet? 104.86.110.241

What is the packet length of the first browser acknowledgement of the SYN ACK response from the markangel webserver? 54bytes

What is the packet length and info of the first communication in the TLS handshake? 430 byte

IP Address of the Web Server Hosting Markangel Stores: 63.250.43.1

This is the destination IP address contacted by the client machine when attempting to access the Markangel Stores web service. It represents the web server hosting the site and is critical for identifying the target server of interest during traffic inspection or incident investigation

Markangel_packet_capture.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

dns.flags.response == 1 && dns.qry.name contains "markangel"

No.	Time	Source	Source port	Destination	Destination port	Protocol	Length	Info
805	2024-10-26 11:15:17.474136	10.10.10.1	53	10.10.10.162	58937	DNS	111	Standard query response 0x5eb6 A mark

> Internet Protocol Version 4, Src: 10.10.10.1, Dst: 10.10.10.162

> User Datagram Protocol, Src Port: 53, Dst Port: 58937

> Domain Name System (response)

Transaction ID: 0x5eb6

Flags: 0x8180 Standard query response, No error

Questions: 1

Answer RRs: 2

Authority RRs: 0

Additional RRs: 0

> Queries

> Answers

markangelstores.com: type A, class IN, addr 63.250.43.1

markangelstores.com: type A, class IN, addr 63.250.43.2

[Request In: 779]

[Time: 0.117719000 seconds]

0000 74 e5 f9 a3 bd ee d4 01 c3 47 e3 ae 08 00 45 00 t.....G....E

0010 00 61 11 b9 00 00 40 11 40 1d 0a 0a 01 0a 0a a.....@.....

0020 0a a2 00 35 e6 39 00 4d 0d 5f 5e b6 81 80 00 01 ..5.9.M.....^....

0030 00 02 00 00 00 00 0f 6d 61 72 6b 61 6e 67 65 6cm arkange

0040 73 74 6f 72 65 73 03 63 6f 6d 00 00 01 00 01 c0 stores.c om.....

0050 0c 00 01 00 01 00 00 00 3c 00 04 3f fa 2b 01 c0<...?..+..

0060 0c 00 01 00 01 00 00 00 3c 00 04 3f fa 2b 02<...?..+..

Markangel_packet_capture.pcapng

26°C Cloudy

Search

Packets: 6631 - Displayed: 1 (0.0%)

Profile: Wireshark Master Class

2:52 PM 8/1/2025

IP Address of the Machine Used to Access the Markangel Website: 10.10.10.162

This is the source IP address observed in the packet capture, which is likely to belong to a device within a private internal network. It identifies the device initiating the request to the Markangel web server. This helps trace user activity or infected endpoints in an investigation

The image shows a Wireshark packet capture analysis. The top pane displays a list of captured packets. The bottom pane shows a detailed view of packet 813, which is a TCP SYN packet from 10.10.10.162 to 63.250.43.1.

No.	Time	Source	Source port	Destination	Destination port	Protocol	Length	Info
6285	2024-10-26 11:15:28.925930	63.250.43.1	443	10.10.10.162	60068	TLSv1.3	1411	[TCP Previous segment not captured]
6286	2024-10-26 11:15:28.925930	63.250.43.1	443	10.10.10.162	60068	TCP	1514	[TCP Out-Of-Order] 443 → 60068 [ACK]
6317	2024-10-26 11:15:28.927142	63.250.43.1	443	10.10.10.162	60068	TCP	1514	[TCP Out-Of-Order] 443 → 60068 [ACK]
6318	2024-10-26 11:15:28.927142	63.250.43.1	443	10.10.10.162	60068	TCP	1514	[TCP Out-Of-Order] 443 → 60068 [ACK]
6319	2024-10-26 11:15:28.927142	63.250.43.1	443	10.10.10.162	60068	TCP	1514	[TCP Out-Of-Order] 443 → 60068 [ACK]
6320	2024-10-26 11:15:28.927142	63.250.43.1	443	10.10.10.162	60068	TCP	1514	[TCP Out-Of-Order] 443 → 60068 [ACK]
813	2024-10-26 11:15:17.486013	10.10.10.162	60068	63.250.43.1	443	TCP	66	60068 → 443 [SYN] Seq=0 Win=64240 Len=0
897	2024-10-26 11:15:17.790378	10.10.10.162	60068	63.250.43.1	443	TCP	54	60068 → 443 [ACK] Seq=1 Ack=1 Win=13
898	2024-10-26 11:15:17.791021	10.10.10.162	60068	63.250.43.1	443	TCP	1474	60068 → 443 [ACK] Seq=1 Ack=1 Win=13
899	2024-10-26 11:15:17.791021	10.10.10.162	60068	63.250.43.1	443	TLSv1.3	395	Client Hello (SNI=markangelstores.co
944	2024-10-26 11:15:18.080717	10.10.10.162	60068	63.250.43.1	443	TCP	54	60068 → 443 [ACK] Seq=1762 Ack=4097
946	2024-10-26 11:15:18.085917	10.10.10.162	60068	63.250.43.1	443	TCP	54	60068 → 443 [ACK] Seq=1762 Ack=5242
947	2024-10-26 11:15:18.103200	10.10.10.162	60068	63.250.43.1	443	TLSv1.3	118	Change Cipher Spec, Application Data
948	2024-10-26 11:15:18.103495	10.10.10.162	60068	63.250.43.1	443	TLSv1.3	146	Application Data

Frame 813: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on
Ethernet II, Src: Intel_a3:bd:ee (74:e5:f9:a3:bd:ee), Dst: Routerboardc_
Internet Protocol Version 4, Src: 10.10.10.162, Dst: 63.250.43.1
Transmission Control Protocol, Src Port: 60068, Dst Port: 443, Seq: 0, L

0000 d4 01 c3 47 e3 ae 74 e5 f9 a3 bd ee 08 00 45 00 ...G...t...
0010 00 34 12 3b 40 00 80 06 68 e2 0a 0a a2 3f fa ...4...h...
0020 2b 01 ea a4 01 bb a0 ff a5 31 00 00 00 00 80 02 +...1...
0030 fa f0 c1 e7 00 00 02 04 05 b4 01 03 03 08 01 01 ...
0040 04 02

Timestamp of the TCP Synchronization (SYN) Request: 2024-10-26 11:15:17.486013

This timestamp marks the exact moment the client initiated a TCP three-way handshake to the Markangel web server. It is useful for creating a timeline of activity, identifying when a session began, and correlating with other system or application logs for deeper analysis.

Markangel_packet_capture.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags.syn == 1 && tcp.flags.ack == 0

No.	Time	Source	Source port	Destination	Destination port	Protocol	Length	Info
189	2024-10-26 11:15:12.453228	10.10.10.162	60063	216.58.223.196	443	TCP	66	60063 → 443 [SYN] Seq=0 Win=64240 Le
330	2024-10-26 11:15:13.519520	10.10.10.162	60064	216.58.223.202	443	TCP	66	60064 → 443 [SYN] Seq=0 Win=64240 Le
448	2024-10-26 11:15:14.463510	10.10.10.162	60065	216.58.223.238	443	TCP	66	60065 → 443 [SYN] Seq=0 Win=64240 Le
475	2024-10-26 11:15:14.554377	10.10.10.162	60066	13.248.221.112	443	TCP	66	60066 → 443 [SYN] Seq=0 Win=64240 Le
642	2024-10-26 11:15:16.244920	10.10.10.162	60067	216.58.223.238	443	TCP	66	60067 → 443 [SYN] Seq=0 Win=64240 Le
813	2024-10-26 11:15:17.486013	10.10.10.162	60068	63.250.43.1	443	TCP	66	60068 → 443 [SYN] Seq=0 Win=64240 Le
815	2024-10-26 11:15:17.501562	10.10.10.162	60069	216.58.223.206	443	TCP	66	60069 → 443 [SYN] Seq=0 Win=64240 Le
893	2024-10-26 11:15:17.738140	10.10.10.162	60070	63.250.43.1	443	TCP	66	60070 → 443 [SYN] Seq=0 Win=64240 Le
1065	2024-10-26 11:15:19.549435	10.10.10.162	60071	216.58.223.196	443	TCP	66	60071 → 443 [SYN] Seq=0 Win=64240 Le
1067	2024-10-26 11:15:19.589419	10.10.10.162	60072	142.250.201.74	443	TCP	66	60072 → 443 [SYN] Seq=0 Win=64240 Le
1086	2024-10-26 11:15:19.717099	10.10.10.162	60073	35.190.80.1	443	TCP	66	60073 → 443 [SYN] Seq=0 Win=64240 Le
1252	2024-10-26 11:15:20.036622	10.10.10.162	60074	104.86.110.241	80	TCP	66	60074 → 80 [SYN] Seq=0 Win=64240 Len
1413	2024-10-26 11:15:20.277146	10.10.10.162	60075	13.107.246.56	443	TCP	66	60075 → 443 [SYN] Seq=0 Win=64240 Le
1533	2024-10-26 11:15:20.512964	10.10.10.162	60076	63.250.43.1	443	TCP	66	60076 → 443 [SYN] Seq=0 Win=64240 Le

> Frame 813: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on

> Ethernet II, Src: Intel_a3:bd:ee (74:e5:f9:a3:bd:ee), Dst: Routerboardc_

> Internet Protocol Version 4, Src: 10.10.10.162, Dst: 63.250.43.1

> Transmission Control Protocol, Src Port: 60068, Dst Port: 443, Seq: 0, L

0000 d4 01 c3 47 e3 ae 74 e5 f9 a3 bd ee 08 00 45 00 ...G...t.....

0010 00 34 12 3b 40 00 80 06 68 e2 0a 0a 0a a2 3f fa -4;@...h.....

0020 2b 01 ea a4 01 bb a0 ff a5 31 00 00 00 80 02 +.....1.....

0030 fa f0 c1 e7 00 00 02 04 05 b4 01 03 03 08 01 01

0040 04 02 ..

Markangel_packet_capture.pcapng

Packets: 6631 / Displayed: 33 (0.5%)

Profile: Wireshark Master Class

26°C

3:32 PM

Source IP of the First SYN-ACK Packet: 104.86.110.241

This IP is the actual source of the SYN-ACK response, indicating the server endpoint that responded to the client. It may reflect a CDN (Content Delivery Network) or a load-balanced proxy in front of the actual Markangel server. This highlights the infrastructure setup and redirection path used in web hosting.

Markangel_packet_capture.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags.syn == 1 && !tcp.flags.ack == 1

No.	Time	Source	Source port	Destination	Destination port	Protocol	Length	Info
1396	2024-10-26 11:15:20.162063	104.86.110.241	80	10.10.10.162	60074	TCP	66	80 → 60074 [SYN, ACK] Seq=0 Ack=1 Wi
4406	2024-10-26 11:15:27.252608	88.221.134.73	80	10.10.10.162	60096	TCP	66	80 → 60096 [SYN, ACK] Seq=0 Ack=1 Wi
197	2024-10-26 11:15:12.492031	216.58.223.196	443	10.10.10.162	60063	TCP	66	443 → 60063 [SYN, ACK] Seq=0 Ack=1 Wi
333	2024-10-26 11:15:13.556400	216.58.223.202	443	10.10.10.162	60064	TCP	66	443 → 60064 [SYN, ACK] Seq=0 Ack=1 Wi
453	2024-10-26 11:15:14.496908	216.58.223.238	443	10.10.10.162	60065	TCP	66	443 → 60065 [SYN, ACK] Seq=0 Ack=1 Wi
476	2024-10-26 11:15:14.586885	13.248.221.112	443	10.10.10.162	60066	TCP	66	443 → 60066 [SYN, ACK] Seq=0 Ack=1 Wi
643	2024-10-26 11:15:16.269032	216.58.223.238	443	10.10.10.162	60067	TCP	66	443 → 60067 [SYN, ACK] Seq=0 Ack=1 Wi
832	2024-10-26 11:15:17.527317	216.58.223.206	443	10.10.10.162	60069	TCP	66	443 → 60069 [SYN, ACK] Seq=0 Ack=1 Wi
896	2024-10-26 11:15:17.790261	63.250.43.1	443	10.10.10.162	60068	TCP	66	443 → 60068 [SYN, ACK] Seq=0 Ack=1 Wi
934	2024-10-26 11:15:18.016477	63.250.43.1	443	10.10.10.162	60070	TCP	66	443 → 60070 [SYN, ACK] Seq=0 Ack=1 Wi
1068	2024-10-26 11:15:19.590583	216.58.223.196	443	10.10.10.162	60071	TCP	66	443 → 60071 [SYN, ACK] Seq=0 Ack=1 Wi
1081	2024-10-26 11:15:19.699345	142.250.201.74	443	10.10.10.162	60072	TCP	66	443 → 60072 [SYN, ACK] Seq=0 Ack=1 Wi
1103	2024-10-26 11:15:19.748019	35.190.80.1	443	10.10.10.162	60073	TCP	66	443 → 60073 [SYN, ACK] Seq=0 Ack=1 Wi
1420	2024-10-26 11:15:20.374193	13.107.246.56	443	10.10.10.162	60075	TCP	66	443 → 60075 [SYN, ACK] Seq=0 Ack=1 Wi

> Frame 1396: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on

> Ethernet II, Src: Routerboardc_47:e3:ae (d4:01:c3:47:e3:ae), Dst: Intel

> Internet Protocol Version 4, Src: 104.86.110.241, Dst: 10.10.10.162

> Transmission Control Protocol, Src Port: 80, Dst Port: 60074, Seq: 0, Ac

0000 74 e5 f9 a3 bd ee d4 01 c3 47 e3 ae 08 00 45 00 t...G...f

0010 00 34 00 00 40 00 36 06 58 d1 68 56 6e f1 0a 0a .-...@ 6 X hVn..

0020 0a a2 00 50 ea aa 5e 8b 6d 87 a3 34 a8 f6 80 12 ...P...^ m 4...

0030 fa f0 84 e4 00 00 02 04 05 b4 01 01 04 02 01 03

0040 03 07

Markangel_packet_capture.pcapng

26°C Cloudy

Search

Packets: 6631 · Displayed: 33 (0.5%)

Profile: Wireshark Master Class

3:33 PM 8/3/2025

Packet Length of First Browser Acknowledgement (ACK): 54 bytes

The 54-byte ACK packet from the client confirms receipt of the SYN-ACK, completing the TCP handshake. Although small, this packet is crucial for session establishment and offers valuable insights into the normal flow of communication initiation.

Markangel_packet_capture.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.flags.ack == 1 && tcp.flags.syn == 0

No.	Time	Source	Source port	Destination	Destination port	Protocol	Length	Info
686	2024-10-26 11:15:16.406750	10.10.10.162	60067	216.58.223.238	443	TLSv1.3	128	Change Cipher Spec, Application Data
697	2024-10-26 11:15:16.492026	10.10.10.162	60067	216.58.223.238	443	TCP	54	60067 → 443 [ACK] Seq=1811 Ack=6379
735	2024-10-26 11:15:17.208278	10.10.10.162	60067	216.58.223.238	443	TCP	54	60067 → 443 [FIN, ACK] Seq=1811 Ack=
761	2024-10-26 11:15:17.246339	10.10.10.162	60067	216.58.223.238	443	TCP	54	60067 → 443 [ACK] Seq=1812 Ack=6380
897	2024-10-26 11:15:17.790378	10.10.10.162	60068	63.250.43.1	443	TCP	54	60068 → 443 [ACK] Seq=1 Ack=1 Win=13
898	2024-10-26 11:15:17.791021	10.10.10.162	60068	63.250.43.1	443	TCP	1474	60068 → 443 [ACK] Seq=1 Ack=1 Win=13
899	2024-10-26 11:15:17.791021	10.10.10.162	60068	63.250.43.1	443	TLSv1.3	395	Client Hello (SNI=markangelstores.co
944	2024-10-26 11:15:18.080717	10.10.10.162	60068	63.250.43.1	443	TCP	54	60068 → 443 [ACK] Seq=1762 Ack=4097
946	2024-10-26 11:15:18.085917	10.10.10.162	60068	63.250.43.1	443	TCP	54	60068 → 443 [ACK] Seq=1762 Ack=5242
947	2024-10-26 11:15:18.103200	10.10.10.162	60068	63.250.43.1	443	TLSv1.3	118	Change Cipher Spec, Application Data
948	2024-10-26 11:15:18.103495	10.10.10.162	60068	63.250.43.1	443	TLSv1.3	146	Application Data
949	2024-10-26 11:15:18.103777	10.10.10.162	60068	63.250.43.1	443	TLSv1.3	955	Application Data
969	2024-10-26 11:15:18.375771	10.10.10.162	60068	63.250.43.1	443	TCP	54	60068 → 443 [ACK] Seq=2819 Ack=5458
970	2024-10-26 11:15:18.375989	10.10.10.162	60068	63.250.43.1	443	TLSv1.3	85	Application Data

> Interface id: 0 (\Device\NPF_{683CD909-2B8F-4E76-9F6C-F603985DF527})

Encapsulation type: Ethernet (1)

Arrival Time: Oct 26, 2024 11:15:17.790378000 W. Central Africa Stand

UTC Arrival Time: Oct 26, 2024 10:15:17.790378000 UTC

Epoch Arrival Time: 1729937717.790378000

[Time shift for this packet: 0.000000000 seconds]

[Time delta from previous captured frame: 0.000117000 seconds]

[Time delta from previous displayed frame: 0.028153000 seconds]

[Time since reference or first frame: 9.985100000 seconds]

Frame Number: 897

Frame Length: 54 bytes (432 bits)

Capture Length: 54 bytes (432 bits)

[Frame is marked: False]

[Frame is ignored: False]

[Protocols in frame: eth:ethertype:ip:tcp]

0000 d4 01 c3 47 e3 ae 74 e5 f9 a3 bd ee 08 00 45 00 ...G..t.....

0010 00 28 12 3d 40 00 80 06 68 ec 0a 0a 0a a2 3f fa ...(-@...h.....

0020 2b 01 ea a4 01 bb a0 ff a5 32 3c 7b c2 f7 50 10 ...+.....2<{...f

0030 02 03 fc 25 00 00 ...%..

AW01 -130%

Search

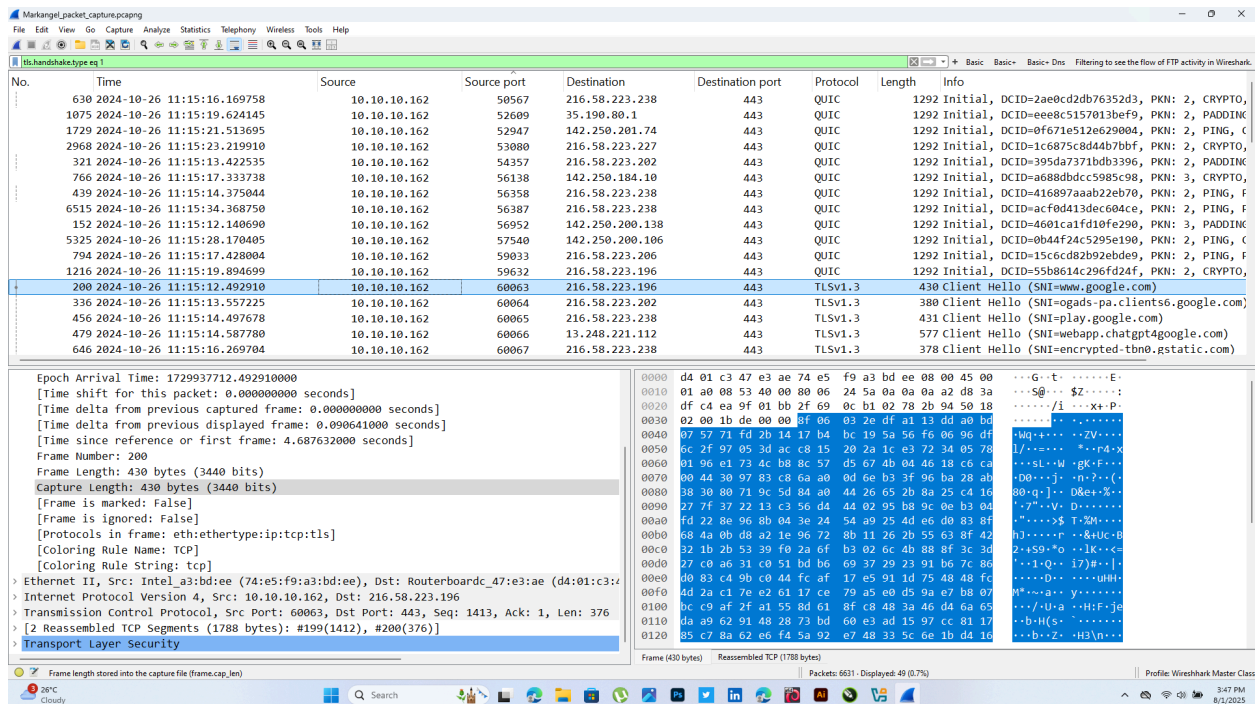
Packets: 6631 · Displayed: 5862 (88.4%)

Profile: Wireshark Master Class

3:40 PM 8/1/2025

Packet Length and Info of First TLS Handshake Communication: 430 bytes

The initial packet in the TLS handshake from the client is 430 bytes and typically contains the Client Hello message. This begins the encrypted session setup and may include the TLS version, supported cypher suites, and extensions. It signifies the transition from plain TCP to encrypted HTTPS traffic.



The screenshot displays a Wireshark packet capture of a TLS handshake. The packet list shows a Client Hello packet (No. 200) with a length of 430 bytes. The packet details pane shows the Client Hello structure, including the epoch arrival time, frame number, and frame length. The packet bytes pane shows the raw data of the Client Hello message.

No.	Time	Source	Source port	Destination	Destination port	Protocol	Length	Info
630	2024-10-26 11:15:16.169758	10.10.10.162	50567	216.58.223.238	443	QUIC	1292	Initial, DCID=2ae0cd2db76352d3, PKN: 2, CRYPTO,
1075	2024-10-26 11:15:19.624145	10.10.10.162	52609	35.190.80.1	443	QUIC	1292	Initial, DCID=eee8c5157013bef9, PKN: 2, PADDING,
1729	2024-10-26 11:15:21.513695	10.10.10.162	52947	142.250.201.74	443	QUIC	1292	Initial, DCID=0f671e512e629804, PKN: 2, PING, C
2968	2024-10-26 11:15:23.219190	10.10.10.162	53080	216.58.223.227	443	QUIC	1292	Initial, DCID=1c6875c8d44b7bbf, PKN: 2, CRYPTO,
321	2024-10-26 11:15:13.422535	10.10.10.162	54357	216.58.223.202	443	QUIC	1292	Initial, DCID=395da7371bdb3396, PKN: 2, PADDING,
766	2024-10-26 11:15:17.333738	10.10.10.162	56138	142.250.184.10	443	QUIC	1292	Initial, DCID=a688dbdc5985c98, PKN: 3, CRYPTO,
439	2024-10-26 11:15:14.375044	10.10.10.162	56358	216.58.223.238	443	QUIC	1292	Initial, DCID=416897aab22eb70, PKN: 2, PING, F
6515	2024-10-26 11:15:34.368750	10.10.10.162	56387	216.58.223.238	443	QUIC	1292	Initial, DCID=acfd413dec604ce, PKN: 2, PING, F
152	2024-10-26 11:15:12.140690	10.10.10.162	56952	142.250.200.138	443	QUIC	1292	Initial, DCID=4601cafd10fe290, PKN: 3, PADDING,
5325	2024-10-26 11:15:28.170405	10.10.10.162	57540	142.250.200.106	443	QUIC	1292	Initial, DCID=0b44f24c5295e190, PKN: 2, PING, C
794	2024-10-26 11:15:17.428004	10.10.10.162	59033	216.58.223.206	443	QUIC	1292	Initial, DCID=15c6cd82b92ebde9, PKN: 2, PING, F
1216	2024-10-26 11:15:19.894699	10.10.10.162	59632	216.58.223.196	443	QUIC	1292	Initial, DCID=55b8614c296fd24f, PKN: 2, CRYPTO,
200	2024-10-26 11:15:12.492910	10.10.10.162	60063	216.58.223.196	443	TLSv1.3	430	Client Hello (SNI=www.google.com)
336	2024-10-26 11:15:13.557225	10.10.10.162	60064	216.58.223.202	443	TLSv1.3	380	Client Hello (SNI=ogads-pa.clients6.google.com)
456	2024-10-26 11:15:14.497678	10.10.10.162	60065	216.58.223.238	443	TLSv1.3	431	Client Hello (SNI=play.google.com)
479	2024-10-26 11:15:14.587780	10.10.10.162	60066	13.248.221.112	443	TLSv1.3	577	Client Hello (SNI=webapp.chatgpt4.google.com)
646	2024-10-26 11:15:16.269704	10.10.10.162	60067	216.58.223.238	443	TLSv1.3	378	Client Hello (SNI=encrypted-tbn0.gstatic.com)

Epoch Arrival Time: 1729937712.492910000
[Time shift for this packet: 0.000000000 seconds]
[Time delta from previous captured frame: 0.000000000 seconds]
[Time delta from previous displayed frame: 0.090641000 seconds]
[Time since reference or first frame: 4.687632000 seconds]
Frame Number: 200
Frame Length: 430 bytes (3440 bits)
Capture Length: 430 bytes (3440 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: ethertype:ip:tcp:tls]
[Coloring Rule Name: TCP]
[Coloring Rule String: tcp]
Ethernet II, Src: Intel_a3:bd:ee (74:e5:f9:a3:bd:ee), Dst: Routerboard_47:e3:ae (d4:01:c3:44:00:00), Protocol: 6, Src Port: 60063, Dst Port: 443, Seq: 1413, Ack: 1, Len: 376
[2 Reassembled TCP Segments (1788 bytes): #199(1412), #200(376)]
Transport Layer Security

0000 d4 01 c3 47 e3 ae 74 e5 f9 a3 bd ee 08 00 45 00 ...G...t...E...
0010 01 a0 08 53 40 00 80 06 24 5a 0a 0a a2 d8 3a ...S...\$Z...:
0020 df c4 ea 9f 01 bb 2f 69 0c b1 02 78 2b 94 50 18/i...x+P...
0030 02 00 1b de 00 00 8f 06 03 2e df a1 13 dd a0 bd ...:....:....
0040 07 57 71 fd 2b 14 17 b4 bc 19 5a 56 f6 06 96 df ...Wq....:ZV...
0050 0c 2f 97 05 3d ac c8 15 20 2a 1c e3 72 34 05 78 1/.....*r4-x
0060 01 96 e1 73 4c b8 c8 57 d5 67 ab 04 46 18 c6 ca ...sL...WgkF...
0070 00 44 30 97 83 c8 6a a0 0d 6e b3 3f 96 ba 28 ab ...D0...j...n?..(
0080 38 30 80 71 9c 5d 84 a0 44 26 65 2b 8a 25 c4 16 80-q-]-D&e+%-
0090 27 7f 37 22 13 c3 56 d4 44 02 95 b8 9c 0e b3 04 ...?..v.v.D.....
00a0 fd 22 8e 9b 80 04 3e 24 54 a9 25 4d e0 d0 83 8f ...>...\$T...
00b0 38 4b 0b d9 a2 1e 96 72 8b 11 26 2b 55 63 8f a2 h.....r...&u...
00c0 22 1b 2b 53 39 f0 2a 6f b3 02 6c 4b 88 8f 3c 3d 2+ASp*o...lk+<
00d0 27 c0 a6 31 c0 51 bd b6 69 37 29 23 91 b6 7c 86 ...1-Q...17...|...
00e0 00 83 c4 9b c0 44 fc af 17 e5 91 1d 75 48 48 fd ...D...U...
00f0 4d 2a c1 7e e2 61 17 ce 79 a5 e0 d5 9a e7 b8 07 M*...a...y.....
0100 bc c9 af 2f a1 55 8d 61 8f c8 48 3a 46 d4 6a 65 .../..u..a...H:F:j...
0110 da a9 62 91 48 28 73 bd 60 e3 ad 15 97 cc 81 17 ...b-H(s...:.....
0120 85 c7 8a 62 e6 f4 5a 92 e7 48 33 5c 6e 1b d4 16 ...b..Z...H3(n...
Frame (430 bytes) Reassembled TCP (1788 bytes) Packets: 6631 - Displayed: 49 (0.7%) Profile: Wireshark Master Class

Conclusion

The network traffic analysis reveals a standard, well-structured communication session between a client device (IP: 10.10.10.162) and the Markangel Stores web server (63.250.43.1). The TCP three-way handshake was completed, with the first SYN initiated at 2024-10-26 11:15:17.486013 and a SYN-ACK response from 104.86.110.241, indicating possible use of a CDN or load balancer.

The handshake was followed by a proper TLS handshake, with the initial Client Hello packet being 430 bytes in size, signalling the start of

encrypted communication. All observed packet lengths and timestamps align with normal browser-based web access behaviour, with no evidence of malicious payloads, unusual port usage, or packet anomalies.

This analysis provides a clear baseline for typical secure client-server interaction over HTTPS and can be referenced for future anomaly detection, behavioural baselining, or threat hunting activities.